REMARKS/ARGUMENTS

The Applicants hereby thank the Examiner for withdrawing the previous grounds for objection and rejection, as well as for the observations in the outstanding Office Action. Claims 3-8 are herein canceled, without prejudice, Claims 1, 2, 9-12, and 14-20 are herein amended, and Claims 21-27 are herein newly added to better encompass the present invention, notwithstanding the Applicants' belief that the Claims would have been allowable as originally filed. The Applicants respectfully assert that no claim has been narrowed within the meaning of *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.* (Fed.Cir. November 29, 2000). By way of the foregoing amendment, the Applicants have made a diligent effort to place the claims in condition for allowance and, alternatively, in condition for appeal. Thus, reconsideration of the Claims in view of the foregoing amendment and these remarks is respectfully requested. However, should any remaining issues be outstanding, the Examiner is respectfully requested to telephone Mr. Thomas F. Lebens at (805) 781-2865 so that such issues may be expeditiously resolved.

I. Rejection of Claims 1, 2, 9-12, 15, 16, and 18 under 35 U.S.C. § 103(a)

Claims 1, 2, 9-12, 15, 16, and 18 stand rejected, under 35 U.S.C. § 103(a), on the grounds of being unpatentable over Paya et al. (US 2004/0181598), in view of Malik et al. (US 7269624), and in further view of Saito et al. (US 2001/0044894). The Applicants respectfully traverse these grounds for rejection on this basis.

Claims 3-8 are herein canceled, without prejudice, thereby rendering moot their grounds for rejection on this basis. Independent Claims 1, 9, 10, and 11 are herein amended generally by inserting the language "incapable of managing a cookie" after "customer device" and by inserting "thereby providing a ubiquitous presence on a network for facilitating provision of a service to the user" at each respective last line. This amendment is believed to be fully supported by the originally filed Specification (p. 1, l. 30 - p. 2, l. 1; p. 4, ll. 1-18; p. 4, l. 30 - p. 5, l. 1; p. 5., ll. 24-27; p. 7, l. 24 - p. 8, l. 5). Dependent Claims 2, 12, 15, 16, and 18 are herein amended only to conform their antecedent bases, to address any informalities, and to economize the language.

With respect to the primary cited reference, Paya et al. merely discloses: "Managing state information across communication sessions between a client and a server via a stateless protocol. The server delivers to the client a cacheable web page with a hyperlink to non-cacheable embedded content. In the hyperlink to the non-cacheable embedded content, the server adds a token or an identifier uniquely associated with the user. When the user obtains embedded content from the cached web page via the hyperlink, the identifier is also sent to the server. Upon receipt of the identifier from the client, the server accesses the stored state information. In this manner, the server manages state information related to the client across communication sessions without the use of cookies as long as the client caches the web page with the unique identifier." (Abstract).

With respect to the secondary cited reference, Malik et al. merely discloses: "A system and method for receiving email instructions allowing users to remotely manage email messages on a specially adapted email server. The adapted email server comprises a registration module and database and other programming logic for verifying the user and determining the user's instructions for managing the email on the server. The user may advantageously manage email messages using any standard email client without the need to actually log in to the server system." (Abstract).

With respect to the tertiary cited reference, Saito et al. merely discloses: "A plurality of application servers, a client, an integrated authentication server and a security information management server are connected to a network. A user having different combinations of user ID's and passwords or certificates for a plurality of kinds of services processed by the plurality of application servers makes requests for services to the individual application servers through the client by using a common integrated certificate. An application server receiving the integrated certificate from the client transfers it to the integrated authentication server. The integrated authentication server checks information of the security information management server to decide whether the right of the user to access the service is valid and when valid, transmits to the application server a combination of a user ID of the user and a password or a certificate

concerning the service. The application server performs user authentication for the user on the basis of the combination of the user ID and the password or the certificate." (Abstract).

In contrast to the cited art, the present invention generally involves the following salient features, *inter alia*: systems, methods, and media for use with a customer device that is "incapable of managing a cookie[,]" "thereby providing a ubiquitous presence on a network for facilitating provision of a service to the user[.]" As such, the Applicants respectfully submit that the cited art does not teach, suggest, motivate, or otherwise obviate the combination of elements and limitations, *inter alia*, as respectively recited by herein amended independent Claims 1, 9, 10, and 11 as follows:

1. A method for computer network access, comprising the steps of:
running a client application, **wherein the client application is not a web browser, and wherein the client application runs on a customer device incapable of managing a cookie;**
entering user information into the customer device;
communicating the entered user information to a first server;
storing the user information on the first server;
creating a unique customer identification for a user of the customer device;
storing the unique customer identification on the first server;
communicating the unique customer identification to a client running the client application and to a plurality of other servers running a plurality of server applications, thereby providing a unique customer identification communication lacking a cookie, wherein the unique customer identification communication is sent to a browser;
storing the unique customer identification on the client server and on the plurality of other servers;
communicating the unique customer identification from the client to at least one server selected from a group consisting essentially of the first server and one other server of the plurality of other servers; and
authenticating the user by matching the unique customer identification received by the at least one server with the unique customer identification stored on the at least one server, **thereby providing a ubiquitous presence on a network for facilitating provision of a service to the user.** [emphasis added]

9. A digital computer system, comprising:
a computer program adapted to:
run a client application **wherein the client application is not a web browser, and wherein the client application runs on a customer device incapable of managing a cookie;**
receive user information entered into the customer device;
communicate the entered user information to a first server;
store the user information on the first server;
create a unique customer identification for a user of the customer device;
store the unique customer identification on the first server;
communicate the unique customer identification to a client running the client application and to a plurality of other servers running a plurality of server applications, whereby a unique customer identification communication is provided, wherein the communication does not include a cookie sent to a browser;

store the unique customer identification on the client and the plurality of other servers;

communicate the unique customer identification from the client to at least one server selected from a group consisting essentially of the first server and one other server of the plurality of other servers; and

authenticate the user by matching the unique customer identification received by the at least one server with the unique customer identification stored on the at least one server or one of the other servers,

wherein each server of the plurality of other servers provides a particular service available to the user of the customer device,

wherein the user prohibited from accessing the service if the unique customer identification received by the at least one server does not match the unique customer identification stored on the at least one server, and

whereby a ubiquitous presence on a network is provided for facilitating provision of a service to the user. [emphasis added]

10. A computer-readable medium, comprising:

a computer program adapted to:

run a client application **wherein the client application is not a web browser, and wherein the client application runs on a customer device incapable of managing a cookie;**

receive user information entered into the customer device;

communicate the entered user information to a first server;

store the user information on the first server;

create a unique customer identification for a user of the customer device;

store the unique customer identification on the first server;

communicate the unique customer identification to a client running the client application and to a plurality of other servers running a plurality of server applications, whereby a unique customer identification communication is provided, wherein the communication does not include a cookie sent to a browser;

store the unique customer identification on the client and the plurality of other servers;

communicate the unique customer identification from the client to at least one server selected from a group consisting essentially of the first server and one other server of the plurality of other servers; and

authenticate the user by matching the unique customer identification received by the at least one server with the unique customer identification stored on the at least one server or one of the other servers,

wherein each server of the plurality of other servers provides a particular service available to the user of the customer device,

wherein the user is prohibited from accessing the service if the unique customer identification received by the at least one server does not match the unique customer identification stored on the at least one server, and

whereby a ubiquitous presence on a network is provided for facilitating provision of a service to the user. [emphasis added]

11. A computer network system, comprising:

a server computer running a server software application operable to create a unique customer identification for a user, store the unique identification on the server computer, communicate the unique customer identification to a client computer, wherein the unique customer identification communication, lacking a cookie, is sent to a browser; and authenticate the user via the unique customer identification when the user communicates with the server computer;

a client computer, incapable of managing a cookie, running a client software application, said client computer being operably connected to the server computer over a network, wherein the client software application is operable to communicate user information to the server

application, store the unique customer identification, and provide the server with the unique customer identification to authenticate a user with the server application; and

at least one additional server computer running an additional server software application, said additional server computer being operably connected to the server computer and client computer over a network, being operable to provide information services to the user, and being operable to receive the unique customer identification from the server computer and to authenticate the user via the unique customer identification when the user communicates with the additional server software application,

whereby a ubiquitous presence on a network is provided for facilitating provision of a service to the user. [emphasis added]

Consequently, Claims 2, 12, 15, 16, and 18 now subsume the limitations of their respective base claims by dependency thereto.

Thus, the Applicants respectfully submit that 1, 2, 9-12, 15, 16, and 18 have not been taught, suggested, motivated, or otherwise obviated by the cited art. Therefore, the Applicants respectfully request that the grounds for rejection on this basis are withdrawn and that Claims 1, 2, 9-12, 15, 16, and 18 are passed to allowance in due course.

II. Rejection of Claims 3-6 under 35 U.S.C. § 103(a)

Claims 3 and 6 stand rejected, under 35 U.S.C. § 103(a), on the grounds of being unpatentable over Paya et al. (US 2004/0181598), in view of Malik et al. (US 7269624) and Saito et al. (US 2001/0044894), and in further view of Gratges, Jr. (US 6324648). The Applicants respectfully traverse these grounds for rejection on this basis. Claims 3 and 6 are herein canceled, without prejudice, thereby rendering moot their grounds for rejection on this basis. Therefore, the Applicants respectfully request that the grounds for rejection on this basis are withdrawn.

III. Rejection of Claims 5 and 8 under 35 U.S.C. § 103(a)

Claims 5 and 8 stand rejected, under 35 U.S.C. § 103(a), on the grounds of being unpatentable over Paya et al. (US 2004/0181598), in view of Malik et al. (US 7269624) and Saito et al. (US 2001/0044894), and in further view of Heimsoth et al. (US 5764915). The Applicants respectfully traverse these grounds for rejection on this basis. Claims 5 and 8 are

herein canceled, without prejudice, thereby rendering moot their grounds for rejection on this basis. Therefore, the Applicants respectfully request that the grounds for rejection on this basis are withdrawn.

IV. Rejection of Claims 4 and 7 under 35 U.S.C. § 103(a)

Claims 4 and 7 stand rejected, under 35 U.S.C. § 103(a), on the grounds of being unpatentable over Paya et al. (US 2004/0181598), in view of Malik et al. (US 7269624) and Saito et al. (US 2001/0044894), and in further view of Lerner et al. (US 2002/0010776). The Applicants respectfully traverse these grounds for rejection on this basis. Claims 4 and 7 are herein canceled, without prejudice, thereby rendering moot their grounds for rejection on this basis. Therefore, the Applicants respectfully request that the grounds for rejection on this basis are withdrawn.

V. Rejection of Claims 14 and 17 under 35 U.S.C. § 103(a)

Claims 14 and 17 stand rejected, under 35 U.S.C. § 103(a), on the grounds of being unpatentable over Paya et al. (US 2004/0181598), in view of Malik et al. (US 7269624) and Saito et al. (US 2001/0044894), and in further view of Fukuda et al. (US 2002/0184539). The Applicants respectfully traverse these grounds for rejection on this basis. Claims 1, 14, and 17 are herein amended, as discussed, *supra*.

As discussed, *supra*, independent Claim 1 is herein amended generally by inserting the language "incapable of managing a cookie" after "customer device" and by inserting "thereby providing a ubiquitous presence on a network for facilitating provision of a service to the user" at each respective last line. This amendment is believed to be fully supported by the originally filed Specification (p. 1, l. 30 - p. 2, l. 1; p. 4, ll. 1-18; p. 4, l. 30 - p. 5, l. 1; p. 5., ll. 24-27; p. 7, l. 24 - p. 8, l. 5). Dependent Claims 14 and 17 are herein amended only to conform their antecedent bases, to address any informalities, and to economize the language.

With respect to the primary cited reference, Paya et al. merely discloses: "Managing state information across communication sessions between a client and a server via a stateless protocol. The server delivers to the client a cacheable web page with a hyperlink to non-cacheable embedded content. In the hyperlink to the non-cacheable embedded content, the server adds a token or an identifier uniquely associated with the user. When the user obtains embedded content from the cached web page via the hyperlink, the identifier is also sent to the server. Upon receipt of the identifier from the client, the server accesses the stored state information. In this manner, the server manages state information related to the client across communication sessions without the use of cookies as long as the client caches the web page with the unique identifier." (Abstract).

With respect to the secondary cited reference, Malik et al. merely discloses: "A system and method for receiving email instructions allowing users to remotely manage email messages on a specially adapted email server. The adapted email server comprises a registration module and database and other programming logic for verifying the user and determining the user's instructions for managing the email on the server. The user may advantageously manage email messages using any standard email client without the need to actually log in to the server system." (Abstract).

With respect to the tertiary cited reference, Saito et al. merely discloses: "A plurality of application servers, a client, an integrated authentication server and a security information management server are connected to a network. A user having different combinations of user ID's and passwords or certificates for a plurality of kinds of services processed by the plurality of application servers makes requests for services to the individual application servers through the client by using a common integrated certificate. An application server receiving the integrated certificate from the client transfers it to the integrated authentication server. The integrated authentication server checks information of the security information management server to decide whether the right of the user to access the service is valid and when valid, transmits to the application server a combination of a user ID of the user and a password or a certificate concerning the service. The application server performs user authentication for the user on the basis of the combination of the user ID and the password or the certificate." (Abstract).

With respect to the quaternary cited reference, Fukuda et al. merely discloses: "An authentication system for authenticating a mobile information terminal is disclosed. The system includes elements for: issuing a user ID to the terminal upon program issuing receipt therefrom; generating a random number based on the user ID and a time of issuing request receipt; registering the random number and the time of receipt in conjunction with the user ID; generating a first program for creating a first image embedded with the user ID, in accordance with the random number, user ID and time of receipt; transmitting the first program to the terminal; picking up the first image displayed on the terminal; recognizing first information from the picked-up first image while extracting the user ID from the same image concurrently; retrieving the registered random number and time of receipt in keeping with the user ID; generating a second program for creating a second image based on the retrieved random number, time of receipt, and user ID; and authenticating the terminal by verifying a match between second information from the second image generated by execution of the second program on the one hand, and the recognized first information on the other hand." (Abstract).

In contrast to the cited art, the present invention generally involves the following salient features, *inter alia*: systems, methods, and media for use with a customer device that is "incapable of managing a cookie[,]" "thereby providing a ubiquitous presence on a network for facilitating provision of a service to the user[.]" As such, the Applicants respectfully submit that the cited art does not teach, suggest, motivate, or otherwise obviate the combination of elements and limitations, *inter alia*, as recited by herein amended independent Claim 1 as follows:

1. A method for computer network access, comprising the steps of:
running a client application, **wherein the client application is not a web browser, and wherein the client application runs on a customer device incapable of managing a cookie**;
entering user information into the customer device;
communicating the entered user information to a first server;
storing the user information on the first server;
creating a unique customer identification for a user of the customer device;
storing the unique customer identification on the first server;
communicating the unique customer identification to a client running the client application and to a plurality of other servers running a plurality of server applications, thereby providing a unique customer identification communication lacking a cookie, wherein the unique customer identification communication is sent to a browser;
storing the unique customer identification on the client server and on the plurality of other servers;
communicating the unique customer identification from the client to at least one server selected from a group consisting essentially of the first server and one other server of the plurality

> of other servers; and
>
> authenticating the user by matching the unique customer identification received by the at least one server with the unique customer identification stored on the at least one server, **thereby providing a ubiquitous presence on a network for facilitating provision of a service to the user.** [emphasis added]

Consequently, Claims 14 and 17 now subsume the limitations of their respective base claims by dependency thereto.

Thus, the Applicants respectfully submit that 14 and 17 have not been taught, suggested, motivated, or otherwise obviated by the cited art. Therefore, the Applicants respectfully request that the grounds for rejection on this basis are withdrawn and that Claims 14 and 17 are passed to allowance in due course.

VI. Rejection of Claims 19 and 20 under 35 U.S.C. § 103(a)

Claims 19 and 20 stand rejected, under 35 U.S.C. § 103(a), on the grounds of being unpatentable over Paya et al. (US 2004/0181598), in view of Malik et al. (US 7269624) and Saito et al. (US 2001/0044894), and in further view of Baker et al. (US 5678041). The Applicants respectfully traverse these grounds for rejection on this basis. Claims 11, 19, and 20 are herein amended, as discussed, *supra*.

As discussed, *supra*, independent Claim 11 is herein amended generally by inserting the language "incapable of managing a cookie" after "customer device" and by inserting "thereby providing a ubiquitous presence on a network for facilitating provision of a service to the user" at each respective last line. This amendment is believed to be fully supported by the originally filed Specification (p. 1, l. 30 - p. 2, l. 1; p. 4, ll. 1-18; p. 4, l. 30 - p. 5, l. 1; p. 5., ll. 24-27; p. 7, l. 24 - p. 8, l. 5). Dependent Claims 19 and 20 are herein amended only to conform their antecedent bases, to address any informalities, and to economize the language.

With respect to the primary cited reference, Paya et al. merely discloses: "Managing state information across communication sessions between a client and a server via a stateless protocol. The server delivers to the client a cacheable web page with a hyperlink to non-

cacheable embedded content. In the hyperlink to the non-cacheable embedded content, the server adds a token or an identifier uniquely associated with the user. When the user obtains embedded content from the cached web page via the hyperlink, the identifier is also sent to the server. Upon receipt of the identifier from the client, the server accesses the stored state information. In this manner, the server manages state information related to the client across communication sessions without the use of cookies as long as the client caches the web page with the unique identifier." (Abstract).

With respect to the secondary cited reference, Malik et al. merely discloses: "A system and method for receiving email instructions allowing users to remotely manage email messages on a specially adapted email server. The adapted email server comprises a registration module and database and other programming logic for verifying the user and determining the user's instructions for managing the email on the server. The user may advantageously manage email messages using any standard email client without the need to actually log in to the server system." (Abstract).

With respect to the tertiary cited reference, Saito et al. merely discloses: "A plurality of application servers, a client, an integrated authentication server and a security information management server are connected to a network. A user having different combinations of user ID's and passwords or certificates for a plurality of kinds of services processed by the plurality of application servers makes requests for services to the individual application servers through the client by using a common integrated certificate. An application server receiving the integrated certificate from the client transfers it to the integrated authentication server. The integrated authentication server checks information of the security information management server to decide whether the right of the user to access the service is valid and when valid, transmits to the application server a combination of a user ID of the user and a password or a certificate concerning the service. The application server performs user authentication for the user on the basis of the combination of the user ID and the password or the certificate." (Abstract).

With respect to the quaternary cited reference, Baker et al. merely discloses: "A system and method for selectively controlling database access by providing a system and method that allows a network administrator or manager to restrict specific system users from accessing

information from certain public or otherwise uncontrolled databases (i.e., the WWW and the Internet). The invention employs a relational database to determine access rights, and this database may be readily updated and modified by an administrator. Within this relational database specific resource identifiers (i.e., URLs) are classified as being in a particular access group. The relational database is arranged so that for each user of the system a request for a particular resource will only be passed on from the local network to a server providing a link to the public/uncontrolled database if the resource identifier is in an access group for which the user has been assigned specific permissions by an administrator. In one preferred embodiment, the invention is implemented as part of a proxy server within the user's local network." (Abstract).

In contrast to the cited art, the present invention generally involves the following salient features, *inter alia*: systems, methods, and media for use with a customer device that is "incapable of managing a cookie[,]" "thereby providing a ubiquitous presence on a network for facilitating provision of a service to the user[.]" As such, the Applicants respectfully submit that the cited art does not teach, suggest, motivate, or otherwise obviate the combination of elements and limitations, *inter alia*, as recited by herein amended independent Claim 11 as follows:

> 11. A computer network system, comprising:
> a server computer running a server software application operable to create a unique customer identification for a user, store the unique identification on the server computer, communicate the unique customer identification to a client computer, wherein the unique customer identification communication, lacking a cookie, is sent to a browser; and authenticate the user via the unique customer identification when the user communicates with the server computer;
> **a client computer, incapable of managing a cookie,** running a client software application, said client computer being operably connected to the server computer over a network, wherein the client software application is operable to communicate user information to the server application, store the unique customer identification, and provide the server with the unique customer identification to authenticate a user with the server application; and
> at least one additional server computer running an additional server software application, said additional server computer being operably connected to the server computer and client computer over a network, being operable to provide information services to the user, and being operable to receive the unique customer identification from the server computer and to authenticate the user via the unique customer identification when the user communicates with the additional server software application,
> **whereby a ubiquitous presence on a network is provided for facilitating provision of a service to the user.** [emphasis added]

Consequently, Claims 19 and 20 now subsume the limitations of their respective base claims by dependency thereto.

Thus, the Applicants respectfully submit that 19 and 20 have not been taught, suggested, motivated, or otherwise obviated by the cited art. Therefore, the Applicants respectfully request that the grounds for rejection on this basis are withdrawn and that Claims 19 and 20 are passed to allowance in due course.

VII. Present Application Pending More than Five Years

Further, the Applicants respectfully submit that the present application has now been pending for over five years, i.e., almost 5.5 years as of the original filing date of **March 19, 2004**. The relevant rules are as follows (MPEP §§ 707.02, 708.01):

707.02 Applications Up for Third Action and 5-Year Applications[R-2]

The supervisory patent examiners should impress their assistants with the fact that the shortest path to the final disposition of an application is by finding the best references on the first search and carefully applying them.

The supervisory patent examiners are expected to personally check on the pendency of every application which is up for the third or subsequent Office Action with a view to finally concluding its prosecution.

Any application that has been pending five years should be carefully studied by the supervisory patent examiner and every effort should be made to terminate its prosecution.

In order to accomplish this result, the application is to be considered "special" by the examiner.

708.01 List of Special Cases [R-2]
37 CFR 1.102 Advancement of examination.

The following is a list of special cases (those which are advanced out of turn for examination):

(A) Applications wherein the inventions are deemed of peculiar importance to some branch of the public service and when for that reason the head of some department of the Government requests immediate action and the *>Director of the USPTO< so orders (37 CFR 1.102).

(B) Applications made special as a result of a petition. (See MPEP § 708.02.)
Subject alone to diligent prosecution by the applicant, an application for patent that has once been made special and advanced out of turn for examination by reason of a ruling made in that particular case (by the Director of the USPTO or a Commissioner) will continue to be special throughout its entire course of prosecution in the U.S. Patent and Trademark Office, including appeal, if any, to the Board of Patent Appeals and Interferences.

(C) Applications for reissues, particularly those involved in stayed litigation (37 CFR 1.176).

(D) Applications remanded by an appellate tribunal for further action.

(E) An application, once taken up for action by an examiner according to its effective filing date, should be treated as special by an examiner, art unit or Technology Center to which it may subsequently be transferred; exemplary situations include new cases transferred as the result of a telephone election and cases transferred as the result of a timely reply to any official action.

(F) Applications which appear to interfere with other applications previously considered and found to be allowable, or which will be placed in interference with an unexpired patent or patents.

(G) Applications ready for allowance, or ready for allowance except as to formal matters.

(H) Applications which are in condition for final rejection.

(I) Applications pending more than 5 years, including those which, by relation to a prior United States application, have an effective pendency of more than 5 years. See MPEP § 707.02.

(J) Reexamination proceedings, MPEP § 2261.

Thus, the Applicants respectfully submit that, since the present application has now been pending for almost 5.5 years as of the original filing date of the present application, the present application should be treated as "special" by the examiner under MPEP §§ 707.02 and 708.01 and that examination of the present application should be advanced. Therefore, the Applicants respectfully request that the grounds for rejection of the Claims on the foregoing bases are withdrawn and that remaining Claims are passed to allowance in due course.

CONCLUSION

Accordingly, Claims 3-8 have been herein canceled, without prejudice, Claims 1, 2, 9-12, and 14-20 have been herein amended, and Claims 21-27 have been herein newly added to better encompass the present invention. The Applicants respectfully reassert that no claim has been narrowed within the meaning of *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.* (Fed.Cir. November 29, 2000). By way of the foregoing amendment, the Applicants believe that the Claims are in condition for allowance. Thus, reconsideration of the remaining Claims in view of the foregoing amendment and remarks is respectfully requested. However, should any remaining issues be outstanding, the Applicants respectfully reiterate the invitation to telephone Mr. Thomas F. Lebens at (805) 781-2865 so that such issues may be resolved as expeditiously as possible. In the event that any additional fees become due or payable, the Examiner is authorized to charge USPTO Deposit Account No. 06-1135 accordingly.

Respectfully submitted,

Dated: 9/8/09

May Lin DeHaan
Reg. No. 42,472
Attorney for the Applicants

Address all correspondence to:
Thomas F. Lebens
FITCH, EVEN, TABIN & FLANNERY
120 South LaSalle, Suite 1600
Chicago, IL 60603

Direct telephone inquiries to:
Thomas F. Lebens
(805) 781-2865